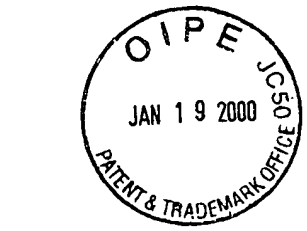
BUNDESREPUBLIK DEUTSCHLAND

09/380412



Bescheinigung

Die DeTeMobil Deutsche Telekom MobilNet GmbH in Bonn/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Zu einem öffentlichen Mobilkommunikationssystem kompartibles Schnurlos-Kommunikationssystem"

am 28. Februar 1997 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole H 04 M und H 04 Q der Internationalen Patentklassifikation erhalten.

München, den 16. September 1999

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Ebert

Aktenzeichen: 197 08 189.4

CERTIFIED COPY OF
PRIORITY DOCUMENT

A 9161
06.90
11/98

28.02.1997
Unser Zeichen: T 97006

Anmelder: DeTeMobil Deutsche Telekom MobilNet GmbH
Landgrabenweg 151, 53227 Bonn

Ansprüche

1. Verfahren zum Betrieb eines Schnurlos-Kommunikationssystems, das auf der Funkschnittstelle mit einem öffentlichen Mobilkommunikationssystem, welches mindestens eine Funktion zur Authentikation aufweist, im wesentlichen kompatibel ist, **dadurch gekennzeichnet**, daß die Basisstation des Schnurlos-Kommunikationssystems mit Einrichtungen zum Lesen und Schreiben von Informationen von/auf Identifikationsmodulen ausgerüstet ist und über eine geeignete Software verfügt, um in Verbindung mit den auf den Identifikationsmodulen abgelegten Daten die Funktionen eines Heimatregisters bzw. einer Berechtigungszentrale bereitzustellen, so daß berechtigte Mobilendgeräte, die sich im Versorgungsgebiet des Schnurlos-Kommunikationssystems befinden, sich bei der ihnen zugehörigen Basisstation authentisieren und einbuchen können.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß wesentliche Bereiche der Daten des in der Basisstation benutzten Identifikationsmoduls identisch mit den auf der Chipkarte (SIM) eines zugangsberechtigten Mobilendgerätes abgelegten Daten ist.

3. Verfahren nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet**, daß vom Netzbetreiber des Mobilkommunikationssystems die Berechtigung des Mobilendgerätes zum Einbuchen bei der Basisstation des Schnurlos-Kommunikationssystems gesperrt werden kann.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, daß auf dem Identifikationsmodul neben individuellen Teilnehmerdaten zur Authentisierung weitere Daten, nämlich die erlaubten Frequenzen, die maximal zulässigen Ausgangsleistungen für die Basisstation und das Mobilendgerät, die zulässigen Dienste (Telefonie, Datenübertragung, Fax etc.) und alle anderen Initialisierungsparameter, auf die der Netzbetreiber Einfluss nehmen will und welche Rahmenvorgabe für den Betrieb der Basisstation des Schnurlos-Systems sind, nicht manipulierbar abgelegt sind.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet**, daß die Funkschnittstelle der Basisstation des Schnurlos-Kommunikationssystems im Frequenzspektrum eines öffentlichen Mobilkommunikationssystems arbeitet.

6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, daß auf der Funkschnittstelle eine Verschlüsselung der übertragenen Daten angewendet wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, daß die Basisstation einen Zeitgeber (Timer) beinhaltet, der vom Netzbetreiber auf eine bestimmte Zeit programmiert ist, und der bei rechtmäßiger Benutzung der Basisstation durch den Teilnehmer immer automatisch zurückgesetzt wird, wobei die Basisstation bei Nichtbenutzung, d.h. nach Ablauf der im Timer programmierten Zeitspanne die Berechtigung verliert, ihren Sender auf den Frequenzen des Mobilkommunikationssystems in Betrieb zu nehmen.

8. Verfahren nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet**, daß bei automatischer Abschaltung der

Basisstation durch Timerablauf die Möglichkeit einer Notwiederaufnahme des Betriebes vorgesehen ist.

9. Verfahren nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet**, daß eine Notwiederaufnahme des Betriebes der Basisstation nur innerhalb eines definierten Zeitfensters möglich ist.

10. Schnurlos-Kommunikationssystem zur Durchführung des Verfahrens gemäß den Ansprüchen 1 bis 9, **dadurch gekennzeichnet**, daß die Basisstation (1) des Schnurlos-Kommunikationssystems mit mindestens einem Lese-/Schreibgerät ausgerüstet ist, mit welchem Informationen üblicher Identifikationsmodule (7) eines öffentlichen Mobilkommunikationssystems gelesen und geschrieben werden können, und in der Basisstation (1) eine geeignete Software implementiert ist, welche Informationen von dem Identifikationsmodul (7) liest bzw. Informationen auf das Identifikationsmodul schreibt und diese verarbeitet.

11. Schnurlos-Kommunikationssystem nach Anspruch 10, **dadurch gekennzeichnet**, daß als Identifikationsmodul (7) die in Mobilkommunikationssystemen üblicherweise benutzten Chipkarten (SIM), wie z.B. nach ISO ID-1, ID-000, DCS 1800, PCS 1900, verwendet werden.

28.02.1997
Unser Zeichen: T 97006

Anmelder: DeTeMobil Deutsche Telekom MobilNet GmbH
Landgrabenweg 151, 53227 Bonn

Zu einem öffentlichen Mobilkommunikationssystem kompatibles Schnurlos-Kommunikationssystem

Die Erfindung betrifft ein zu einem öffentlichen Mobilkommunikationssystem kompatibles Schnurlos-Kommunikationssystem nach dem Oberbegriff des Patentanspruchs 1.

Bei den heutigen mobilen Kommunikationssystemen gibt es eine klare Unterscheidung zwischen Öffentlichen Mobilfunksystemen, wie z.B. dem GSM-System, und privaten Schnurlos-Kommunikationssystemen, die z.B. nach dem digitalen DECT-Standard arbeiten. Dies hat zu unterschiedlichen Gerätesystemen geführt, welche entweder für den Mobilfunkbetrieb oder den Schnurlos-Betrieb geeignet sind.

Es wurden schon Versuche unternommen, Endgeräte, insbesondere Mobilendgeräte, zu konstruieren, welche zum Betrieb in zwei verschiedenen Mobilkommunikationssystemen geeignet sind. Aufgrund der Inkompatibilität der verschiedenen Standards führt dies jedoch zu relativ benutzerunfreundlichen und teueren Lösungen.

Ein anderer Ansatzpunkt liegt darin, die Basisstation eines Schnurlos-Kommunikationssystem derart einzurichten, daß diese zu einem öffentlichen Mobilkommunikationssystem kompatibel ist, d.h. mit herkömmlichen Mobilendgeräten des öffentlichen Mobilkommunikationssystems kommunizieren kann. Es fehlt jedoch an geeigneten Lösungsvorschlägen zur Realisation, z.B.

der erforderlichen Sicherheitsfunktionen. Ein Problem liegt dabei darin, daß die Basisstation des Schnurlos-Kommunikationssystem mit einem leitungsgebundenen Festnetz verbunden ist, so daß eine direkte Beeinflussung der Basisstation über das Mobilkommunikationssystem nicht möglich ist.

Aufgabe der Erfindung ist es daher, ein Schnurlos-Kommunikationssystem mit Sicherheitsfunktionen vorzuschlagen, welches mit einem öffentlichen Mobilkommunikationssystem kompatibel ist und die Benutzung zugehöriger Mobilendgeräte erlaubt.
Eine weitere Aufgabe besteht darin, daß das Schnurlos-Kommunikationssystem trotz seiner Eigenschaft als privates System die Möglichkeit aufweisen soll, unter Kontrolle des jeweiligen Mobilkommunikations-Netzbetreibers eingerichtet und betrieben zu werden.

Zur Lösung der gestellten Aufgabe ist die Erfindung durch die Merkmale des Anspruchs 1 gekennzeichnet.

Das Wesen der Erfindung besteht darin, die Basisstation des Schnurlos-Kommunikationssystems mit einem geeigneten Lese-/Schreibgerät auszustatten, mit welchem Informationen herkömmlicher Identifikationsmodule, darunter werden verstanden z.B. Chipkarten, SIM's (Subsciber Identity Modules), allgmein alle aktiven informationsspeichernden und informationsverarbeitenden Datenträger, gelesen und beschrieben werden können. In Verbindung mit einer geeigneten Software und den auf dem Identifikationsmodul abgelegten Daten ist die Basisstation des Schnurlos-Kommunikationssystems nun in der Lage, die Funktionen einer Basisstation des Mobilkommunikationsnetzes mit Authentifiktionsfunktionalität, genauer, die Funktionen eines Heimatregisters (HLR: Home Location Register) bzw. einer Berechtigungszentrale (AUC: Authentication Center) zu

übernehmen. Damit kann sich jedes zur Benutzung befugte Mobilendgerät bei der Basisstation des Schnurlos-Kommunikationssystems einbuchen und über das Festnetz kommunizieren.

Im folgenden bezieht sich der Begriff „Basisstation", sofern nicht anders angegeben, auf die Basisstation des Schnurlos-Kommunikationssystems.

Im folgenden wird eine von vielen Möglichkeiten des Erfindungsgedankens am Beispiel eines GSM-Mobilkommunikationssystems beschrieben. Die Erfindung ist jedoch nicht auf das GSM-Mobilkommunikationssystem beschränkt.

Mit der Implementierung eines oder mehrerer Chipkartenleser/-schreiber und einer üblichen SIM-Chipkarte in der Basisstation des Schnurlos-Kommunikationssystems wird erreicht, daß der Betrieb der Basisstation unter Kontrolle des jeweiligen GSM-Netzbetreibers arbeitet und daß dem Teilnehmer im „GSM-Schnurlosbetrieb" Sicherheitsmerkmale, wie z.B. Authentikation und Verschlüsselung der Gesprächsdaten, wie beim Betrieb im GSM-Mobilfunknetz geboten werden. Wichtig ist, daß die zum Betrieb der Basisstation benötigte Chipkarte allein durch den Netzbetreiber ausgegeben wird, wie es auch bei GSM-Mobilendgeräten üblich ist.

Die in der Basisstation verwendete Chipkarte übernimmt hierbei zusammen mit einer geeigneten, in der Basisstation implementierten Software die Funktionen des Heimatregisters (HLR) bzw. der Berechtigungszentrale (AUC), das heisst, das Mobilendgerät authentisiert sich nun gegenüber der Basisstation des Schnurlossystems, und nicht, wie gewohnt gegenüber dem Mobilfunknetz. Dabei wird anhand der implementierten Software in der Basisstation eine Zufallszahl generiert, die mit dem in beiden Chipkarten, der Chipkarte

der Basisstation und der Chipkarte des Mobilendgeräts, identisch abgelegten K_i-Schlüssel und dem GSM-systemspezifischen A3-Algorithmus zu je einer SRES-Antwort (Authentisierungsergebnis) umgeformt wird. Bei Übereinstimmung der beiden Authentisierungsergebnisse - der Basisstation und des Mobilendgeräts - ist die Authentifikation erfolgreich. Diese Authentisierungsprozedur gleicht der des GSM-Systems.

Aus der gleichen Zufallszahl wird mit dem K_i-Schlüssel und dem A8-Algorithmus in bekannter Weise der Schlüssel K_c hergeleitet, der zur Verschlüsselung der Kommunikation auf der Funkschnittstelle im Schnurlosbetrieb dient (wie beim GSM-System).

Neben den üblichen personenspezifischen Daten können auf dem SIM der Basisstation noch zusätzliche Daten, wie z.B. die erlaubten Frequenzen, die maximal zulässigen Ausgangsleistungen für die Basisstation und das Mobilendgerät, die zulässigen Dienste (Telefonie, Datenübertragung, Fax etc.) und alle anderen Initialisierungsparameter, auf die der Netzbetreiber Einfluss nehmen will und welche die Basisstation benutzen darf, nicht manipulierbar abgelegt werden. Dies entspricht, zumindest für die Dienste, der bekannten Berechtigungsverwaltung im Heimatregister (HLR) eines GSM-Mobilfunknetzes.

Durch geeignetes Schlüsselmanagement kann erreicht werden, daß mehrere Teilnehmer, z.B. Familienangehörige, über ein und dieselbe Basisstation kommunizieren können. Dazu ist als erste Möglichkeit vorgesehen, daß jeder Teilnehmer, der die Basisstation benutzen will, seine eigene zweite SIM-Karte besitzt, die in die Basisstation eingesteckt werden kann. Die Basisstation benötigt hierfür mehrere Kartenlesegeräte.

Eine andere Möglichkeit besteht darin, daß auf der SIM-Karte der Basisstation Daten und Schlüssel für mehrere Teilnehmer gespeichert sind.
Des weiteren ist ein Gruppenschlüssel in der Basisstation denkbar, der die Authentikation mehrerer individueller Teilnehmer erlaubt.

Wichtig ist, daß die in der Basisstation verwendete Chipkarte im Kernbereich identische Informationen enthält, wie die Chipkarte de GSM-Mobilendgerätes, die mit der Basisstation betrieben werden soll. Nur wenn die persönlichen Benutzerdaten, insbesondere die Sicherheitsfunktionen auf beiden Karten übereinstimmen, kann sich ein Mobilendgerät bei der Basisstation authentisieren und einbuchen.

Bei Kündigung des regulären GSM-Teilnehmerverhältnisses wird in der SIM-Karte des Mobilendgerätes, vorzugsweise über die GSM-Funkschnittstelle, die Berechtigung zum Kommunizieren mit der Basisstation gelöscht. Damit ist ein weiterer Betrieb der Basisstation auf den jeweiligen vom spezifischen Netzbetreiber freigeschalteten Frequenzen nicht mehr sinnvoll möglich, da sich das Mobilendgerät nicht mehr bei der Basisstation authentisieren kann.

Eine mögliche Ausführungsform sieht zudem vor, daß die Basisstation einen Zeitgeber (Timer) beinhaltet, der vom Netzbetreiber auf eine bestimmte Zeit programmiert ist, und bei Benutzung der Basisstation durch den Teilnehmer immer wieder automatisch zurückgesetzt wird. Bei Nichtbenutzung der Basisstation, z.B. nach Kündigung des Teilnehmerverhältnisses, verliert die Basisstation nach Ablauf der programmierten Zeitspanne die Berechtigung, den Sender auf den Frequenzen des Mobilkommunikationssystems in Betrieb zu nehmen. Wird die Basisstation für längere Zeit nicht benutzt, kann die Funktion des Timers durch abschalten der Basisstation eingefroren werden.

Hat der Teilnehmer z.B. vor Antritt eines langen Urlaubs, vergessen, die Basisstation abzuschalten und hat sich diese automatisch deaktiviert, so ist innerhalb eines definierten Zeitfensters die Möglichkeit einer Notwiederaufnahme vorgesehen.

Zur Realisierung einer GSM-kompatiblen Basisstation ist diese zunächst mit einem Kartenleser für GSM-SIM-Karten auszustatten. Weiterhin muß die Basisstation dazu in der Lage sein auf GSM-Standardfrequenzen zu senden und zu empfangen. Die Steuerung der Funktionen der Basisstation erfolgt über eine geeignete Software, wie sie z.B. in den GSM-Endgeräten benutzt wird, und welche die GSM-übliche Authentifikation und weiteren Funktionen durchführt und steuert.

Das Mobilendgerät selbst bedarf nur geringer softwaretechnischer Modifikation.

Figur 1 zeigt schematisch eine beispielhafte physikalische Konstellation des erfindungsgemäßen Systems;

Figur 2 zeigt schematisch eine beispielhafte logische Konstellation des erfindungsgemäßen Systems.

In Figur 1 sind schematisch einige Einrichtungen eines öffentlichen Mobilkommunikationssystems dargestellt. Es ist ein Mobilendgerät 3 vorhanden, welches sich im Versorgungsbereich einer Basisstation 4 des Mobilkommunikationssystems befindet und mit dieser über die Funkschnittstelle verschlüsselt kommunizieren kann. Die Basisstation 4 des Mobilkommunikationssystems ist mit einer Vermittlungsstelle 5 verbunden, die Zugang zu einem öffentlichen Festnetz 9 hat. Weiterhin steht die Vermittlungsstelle 5 mit dem Heimatregister (HLR) und der Berechtigungszentrale (AUC) des Mobilfunknetzes in Kontakt. Will sich das Mobilendgerät 3 im Mobilkommunikationsnetz

einbuchen, so wird in bekannter Weise innerhalb des Heimatregisters bzw. der Berechtigungszentrale 6 eine Authentifikation des Mobilendgerätes 3 durchgeführt.

Des weiteren ist eine ebenfalls mit einem öffentlichen leitungsgebundenen Festnetz 2 (PSTN, ISDN) verbundene Basisstation 1 (HBS) eines Schnurlos-Kommunikationssystems dargestellt. Aufgrund der geringen Ausgangsleistung ist der Versorgungsbereich der Basisstation relativ klein. In der Regel befindet sich die Basisstation 1 innerhalb des Versorgungsbereiches einer oder mehrerer Basisstationen 4 eines öffentlichen Mobilkommunikationsnetzes.

Wie in Figur 2 dargestellt ist, authentisiert sich das Mobilendgerät 3 im Mobilfunkbetrieb über das Mobilfunknetz, und zwar mit Hilfe eines spezifischen Identifikationsschlüssels (K_i-Schlüssel) der einerseits in der SIM-Karte 8 des Mobilendgerätes 3 und andererseits im Heimatregister 6 (HLR) bez. der Berechtigungszentrale (AUC) des Mobilkommunikationssystems abgelegt ist.

Erfindungsgemäß ist nun die Basisstation 1 des Schnurlos-Kommunikationssystems mit einem Identifikationsmodul 7 (z.B. ebenfalls mit einer SIM-Karte) und einer geeigneten Software ausgestattet, um in Verbindung mit den auf dem Identifikationsmodul 7 abgelegten Daten nun dieselben Funktionen und Aufgaben wahrzunehmen, die das Heimatregister bzw. die Berechtigungszentrale des Mobilkommunikationssystems wahrnehmen, so daß das Mobilendgerät 3, sofern es sich im Versorgungsgebiet des Schnurlos-Kommunikationssystems befinden und eine Zugangsberechtigung hat, sich bei der ihr zugehörigen Basisstation 1 des Schnurlossystems authentisieren, einbuchen und verschlüsselt kommunizieren kann.

Das ist nur möglich, wenn wesentliche Bereiche der Daten des in der Basisstation 1 benutzten Identifikationsmoduls 7 identisch mit den auf der Chipkarte (SIM) des zugangsberechtigten Mobilendgerätes 3 abgelegten Daten ist.

Erfindunggemäß ist die Basisstation 1 des Schnurlossystems nun kompatibel zum Mobilkommunikationssystem, d.h. im Standby-Modus sendet die Basisstation 1 des Schnurlossystems periodisch eine spezifische Kennung aus, um seine Anwesenheit und Betriebsbereitschaft anzuzeigen. Das Mobilendgerät 3 hört das Frequenzband nach der spezifischen Kennung der Basisstation 1 ab. Wenn das Mobilendgerät 3 in den Versorgungsbereich der Basisstation 1 kommt, und deren Kennung störungsfrei empfängt, wird das Mobilendgerät 3 versuchen sich in beschriebener Weise bei der Basisstation 1 einzubuchen. Dazu werden, wie beim GSM-System, Authentisierungs- und Initialisierungsnachrichten zwischen Basisstation 1 und Mobilendgerät 3 ausgetauscht. War die Authentisierung erfolgreich kann das Mobilendgerät 3 über das Festnetz 2 kommunizieren, ohne Umweg über das Mobilkommunikationsnetz.

Natürlich ist es auch möglich daß mehrere berechtigte Mobilendgeräte 3 ohne Mitwirkung eines öffentlichen Festnetzes 2, 9 oder des Mobilkommunikationsnetzes über die Basisstation 1 des Schnurlos-Kommunikationsnetzes miteinander verschlüsselt kommunizieren.

Zusammenfassung

Die Erfindung betrifft ein Verfahren zum Betrieb eines Schnurlos-Kommunikationssystems, das auf der Funkschnittstelle mit einem öffentlichen Mobilkommunikationssystem, welches mindestens eine Funktion zur Authentikation aufweist, im wesentlichen kompatibel ist, und eine Vorrichtung zur Durchführung des Verfahrens unter Bereitstellung der Sicherheitsfunktionalität des öffentlichen Mobilkommunikationssystems (Authentisierung, Verschlüsselung).

Dabei ist die Basisstation des Schnurlos-Kommunikationssystems mit Einrichtungen zum Lesen und Schreiben von Informationen von/auf Identifikationsmodulen ausgerüstet und verfügt über eine geeignete Software, um zusammen mit den auf dem Identifikationsmodul abgelegten Daten die Funktionen eines Heimatregisters (HLR) bzw. einer Berechtigungszentrale (AUC) bereitzustellen, so daß berechtigte Mobilendgeräte, die sich im Versorgungsgebiet des Schnurlos-Kommunikationssystems befinden, sich bei der Basisstation des Schnurlossystems authentisieren, einbuchen und verschlüsselt kommunizieren können.

Auf den Identifikationsmodulen werden außerdem noch sämtliche Initialisierungsparameter der Schnurlos-Basisstationen, die der Netzbetreiber unter Kontrolle halten will, nicht manipulierbar abgelegt.

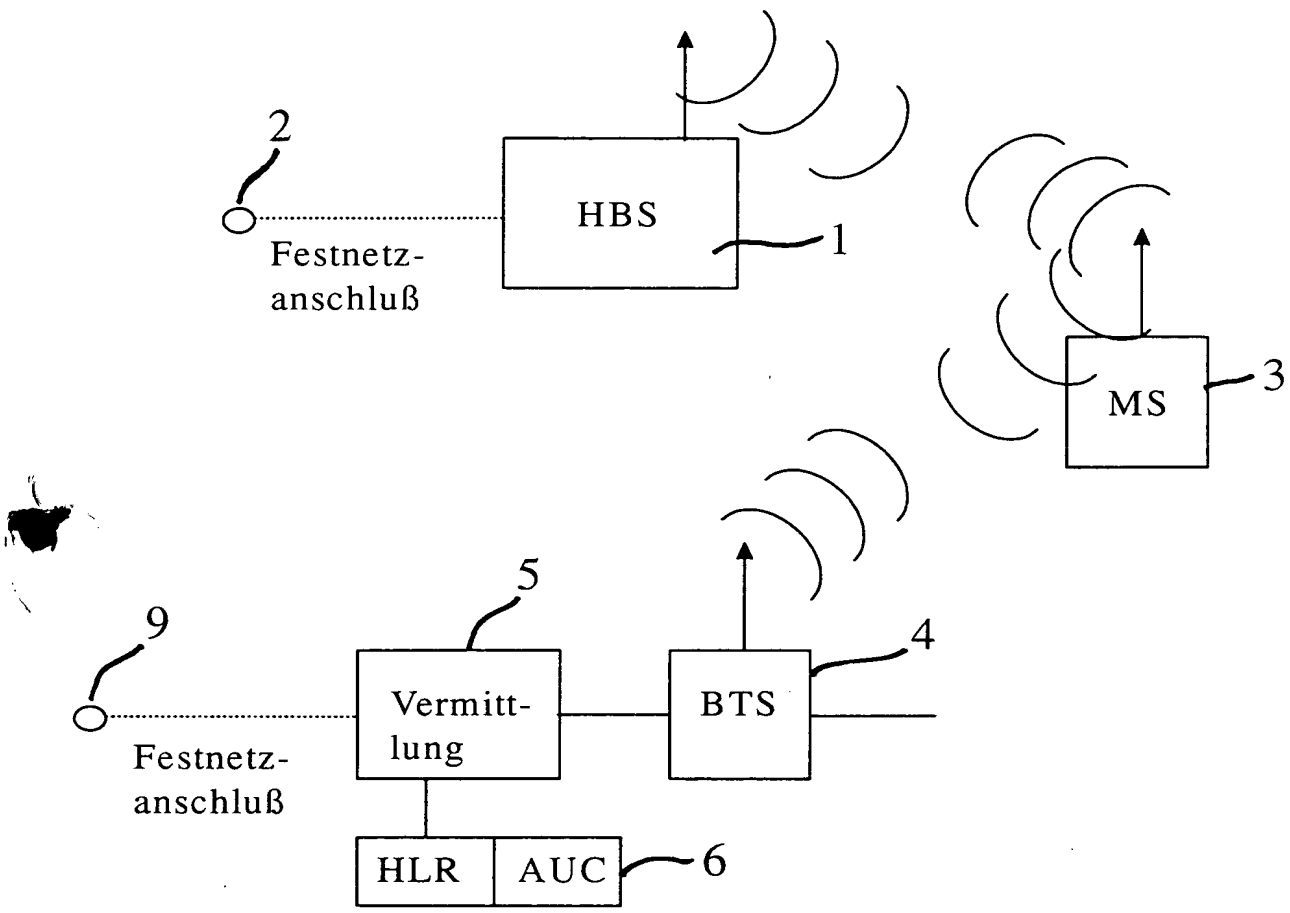


Fig. 1: physikalische Konstellation

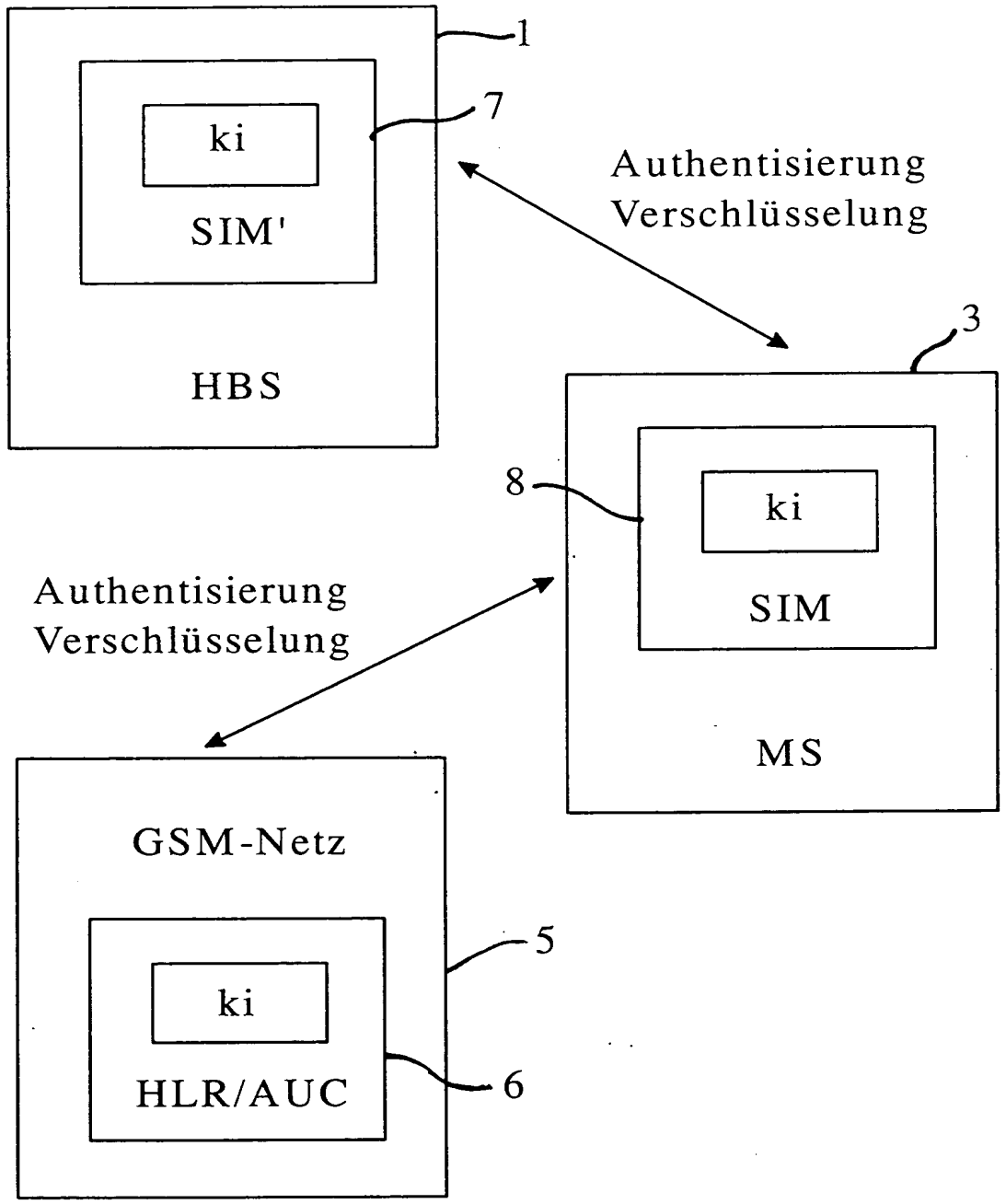


Fig. 2: logische Konstellation